Docket No. YOR920000803US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Bantz et al.**	§	
	§	Group Art Unit: **2134**
Serial No. **09/788,071**	§	
	§	Examiner: **Simitoski, Michael J.**
Filed: **February 16, 2001**	§	
	§	
For: **Apparatus and Methods for Active Avoidance of Objectionable Content**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300, on 12.13.05
By: Amelia C. Turner

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on October 14, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 2, 7-9, 12-15, 18, 23-25, 28-31, 34, 39-41, and 44-47
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48
4. Claims allowed: NONE
5. Claims rejected: 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48
5. Claims objected to: NONE

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48

STATUS OF AMENDMENTS

An amendment after final was filed on September 23, 2005, changing the word "from" to "for" in claims 1, 17, and 33 to correct a clear typographical error. In the Final Office Action issued on July 14, 2005, the Examiner correctly determined that the specification did not provide support for "receiving requested content from a requesting user." The Examiner stated that the phrase "from a requesting user" would be ignored to advance prosecution; therefore, it was not given patentable weight. Clearly, the claim should have recited "receiving a request **for** content **from** a requesting user" or "receiving requested content **for** a requesting user." In the September 23 response, claims 1, 17, and 33 were amended to correct this very superficial error.

In the Advisory Action issued October 24, 2005, the Examiner stated that the above-described amendment would require further consideration and/or search, even though the phrase "for the requesting user" appears in the **very next line** and the effect of the phrase permeates throughout the claim. If any common sense were applied to the interpretation of the claim, there is no way such a superficial amendment could require further consideration or search. Nonetheless, in an interview on November 7, 2005, the Examiner stated that and amendment removing the phrase "from a requesting user" from line 2 of claim 1, and similar amendments to independent claims 17 and 33, would be entered. Therefore, an amendment is filed herewith removing the offending phrase and correcting antecedent basis to reduce issues for appeal. In effect, the new matter objection is overcome and will not be listed in the issues under appeal.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1:

The presently claimed invention provides a method of identifying objectionable content. The present invention retrieves requested content. See specification, page 9, line 8, to page 10, line 21; page 14, line 14. The present invention retrieves a user profile for a requesting user. The user profile includes parameters for identifying objectionable content and a plurality of thresholds including a threshold for each of a plurality of categories of objectionable content. See specification, page 11, line 15, to page 12, line 7; page 14, lines 14 and 15. The present invention analyzes the requested content using the parameters stored in the user profile of the requesting user to identify an amount of objectionable content based on the parameters for each of the plurality of categories of objectionable content. See specification, page 10, line 20, to page 12, line 29. The present invention determines a score for the requested content for each of the plurality of categories of objectionable content based on the amount and category of objectionable content contained in the requested content. See specification, page 12, lines 8-29; page 14, line 15. The present invention stores the requested content in an objectionable content data structure if a score for the requested content is above at least one threshold for at least one category of objectionable content. See specification, page 13, lines 1-24; page 14, lines 17-19.

Independent claim 17:

The presently claimed invention provides an apparatus for identifying objectionable content. The apparatus may be an objectionable content avoidance service provider **106**, which may be implemented as a proxy server in a client **104** or a server **108-112**. The apparatus comprises a first interface, which retrieves requested content. See specification, page 9, line 8, to page 10, line 21; page 14, line 14. The apparatus comprises a user profile for a requesting user. The user profile includes parameters for identifying objectionable content and a plurality of thresholds including a threshold for each of a plurality of categories of objectionable content. See specification, page 11, line 15, to page 12, line 7; page 14, lines 14 and 15. The apparatus comprises a processor which analyzes the requested content using the parameters stored in the

user profile of the requesting user to identify an amount of objectionable content based on the parameters for each of the plurality of categories of objectionable content. See specification, page 10, line 20, to page 12, line 29. The processor determines a score for the requested content for each of the plurality of categories of objectionable content based on the amount and category of objectionable content contained in the requested content. See specification, page 12, lines 8-29; page 14, line 15. The apparatus comprises a storage device, which stores the requested content in an objectionable content data structure if a score for the requested content is above at least one threshold for at least one category of objectionable content. See specification, page 13, lines 1-24; page 14, lines 17-19.

Independent claim 32:

The presently claimed invention provides a computer program product for identifying objectionable content. The present invention retrieves requested content. See specification, page 9, line 8, to page 10, line 21; page 14, line 14. The present invention retrieves a user profile for a requesting user. The user profile includes parameters for identifying objectionable content and a plurality of thresholds including a threshold for each of a plurality of categories of objectionable content. See specification, page 11, line 15, to page 12, line 7; page 14, lines 14 and 15. The present invention analyzes the requested content using the parameters stored in the user profile of the requesting user to identify an amount of objectionable content based on the parameters for each of the plurality of categories of objectionable content. See specification, page 10, line 20, to page 12, line 29. The present invention determines a score for the requested content for each of the plurality of categories of objectionable content based on the amount and category of objectionable content contained in the requested content. See specification, page 12, lines 8-29; page 14, line 15. The present invention stores the requested content in an objectionable content data structure if a score for the requested content is above at least one threshold for at least one category of objectionable content. See specification, page 13, lines 1-24; page 14, lines 17-19. The computer instructions embodied on a computer readable medium are as described with reference to **Figure 5** in the description at page 14, lines 10-20.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection on appeal are as follows:

I. Claims 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over *Hoffberg* (U.S. Patent No. 6,529,942) in view of *Jensen et al.* (U.S. Patent No. 6,459,809).

ARGUMENT

I. 35 U.S.C. § 103, Alleged Obviousness of claims 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48

The Final Office Action rejects claims 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48 under 35 U.S.C. § 103 as allegedly being unpatentable over *Hoffberg* (U.S. Patent No. 6,850,252) in view of *Jensen et al.* (U.S. Patent No. 6,459,809). This rejection is respectfully traversed.

Hoffberg teaches an intelligent electronic appliance. A media metadata processing system analyzes media content to understand the content and generate content-descriptive metadata. See *Hoffberg*, Abstract. The Final Office Action alleges that *Hoffberg* teaches analyzing requested content to identify an amount of objectionable content at col. 143, line 47, through col. 144, line 3, which states:

> In a further embodiment of the present invention, it is an object to provide a device for identifying a program in response to user preference data and program control information concerning available programs, comprising means for gathering the user preference data; means, connected to the gathering means, for storing the gathered user preference data; means for accessing the program control information; and means, connected to the storing means and accessing means, for identifying one or more programs based on a correspondence between a user's programming preferences and the program control information. For example, the identifying means identifies a plurality of programs, a sequence of identifications transmitted to the user being based on a degree of correspondence between a user's programming preferences and the respective program control information of the identified program. The device my selectively record or display the program, or identify the program for the user, who may then define the appropriate action by the device. Therefore, a user may, instead of defining "like" preferences, may define "dislike" preference, which are then used to avoid or filter certain content. Thus, this feature may be used for censoring or parental screening, or merely to avoid unwanted content. Thus, the device comprises a user interface adapted to allow interaction between the user and the device for response to one or more of the identified programs. The device also preferably comprises means for gathering the user specific data comprises means for monitoring a response of the user to identified programs.

Hoffberg appears to teach analyzing content based on a user's likes and dislikes. *Hoffberg* also appears to teach that media content may be correlated based on a predetermined category of media data, such as through an electronic program guide. See *Hoffberg*, col. 222, line 65, to col. 223, line 11. The categories of media data are predetermined and are only used to correlate the media.

The Final Office Action acknowledges that *Hoffberg* does not teach storing the requested content in an objectionable content data structure if the amount of objectionable content in the requested content is above at least one predetermined threshold. However, the Final Office Action alleges that *Jensen* teaches this feature because *Jensen* teaches a dictionary of archtypes.

Jensen teaches searching and filtering content streams using contour transformations. The system and methods of *Jensen* analyze an area of interest and assign a semantic value. With regard to a semantic value, *Jensen* states:

> The semantic value(s) provided by contour transformations are used to position the data set area within a dictionary of archetypes. These archetypal semantic values may have textual or database labels such as "nose", "Upper-Case A", or "snail", assigned to them. Semantic values which characterize one or more archetypes are compared with the semantic values derived from the new data set, to assign the data set to an archetype. If none of the archetypes fit the new data set within specified tolerances, a new archetype may be created with assistance from the user.

Jensen, col. 2, lines 53-62. Thus, a semantic value is used only to categorize an area of interest as an archetype. Semantic values are used to build a dictionary of archetypes. *Jensen* states:

> During the storing step 506, the semantic value produced by the contour transformation and/or associated information is stored within a dictionary of archetypes. This may involve comparing the new semantic value with semantic values for archetypes previously stored in the dictionary. For instance, if the semantic value is in a range or region of values belonging to an existing archetype ("noses" or "starfish", for instance) then the corresponding data set content object (or its address) might be added as one more example of that archetype. If the semantic value is more than a predetermined distance from any existing archetype's semantic value(s) then a new archetype could be added.
>
> Archetype signals are discussed in connection with FIG. 7, but in general they may include one or more semantic values obtained from contour transformations plus a copy of the content object (or a pointer to it); an archetype may also contain a textual

> description or a list of keywords. The present invention can be used in a process which categorizes content and associates keywords with the content to permit subsequent searches using conventional text-based search engines, conventional relational or hierarchical databases, directory services such as Novell's NDS, or the like.

Jensen, col. 9, line 62, to col. 10, line 16. *Jensen* also teaches that some archetypes may be blocked or rerouted. *Jensen* states:

> During the blocking or removing step 508, the semantic value produced by the contour transformation is used to block or reroute at least a portion of a digital data set. The portion may be an individual file, a record in a database, or an entire digital data set, for instance. This step 508 may use a dictionary of archetypes if several objectionable content objects, or several objectionable combinations of individually innocuous objects or features, are to be blocked or rerouted. For instance, a dictionary of archetypes could be used to identify sexually explicit images. However, in some embodiments a complex dictionary is not needed, because only the semantic values themselves and a fixed set of prohibited values are used. If the semantic value for a given portion of the content stream falls within the fixed set of prohibited semantic values, then that portion of the content is blocked or rerouted in a predefined manner. Conventional tools and techniques for preventing further transmission of data and/or rerouting data may be used.

Jensen, col. 10, lines 17-34. Thus, Semantic values are not a score used to quantify an amount of objectionable content. A contour either has a semantic value belonging to an archetype associated with objectionable content or it does not. If the contour or area of interest has a semantic value belonging to an archetype that is to be blocked, then it is blocked.

In contradistinction, the present invention provides a method, apparatus, and computer program product for identifying objectionable content based on an **amount** of objectionable content, as compared to a plurality of thresholds. A user profile includes parameters for identifying objectionable content and **a plurality of thresholds** for a plurality of categories of objectionable content. Content requested by the user is then analyzed using the parameters to identify an amount of objectionable content. A score is determined for each category. If a score for a category is above the threshold for that category, then the objectionable content is stored in an objectionable content data structure.

Neither reference teaches or suggests a plurality of thresholds for a plurality of categories of objectionable content. At best, *Hoffberg* teaches categories of media data. However, *Hoffberg* makes no mention whatsoever of a plurality of categories of **objectionable content** and a corresponding plurality of **thresholds**. The Final Office Action is silent as to this feature. Therefore, the Final Office Action fails to establish a *prima facie* case of obviousness, because the Final Office Action does not show where each and every claim limitation is taught or fairly suggested by the applied prior art.

With respect to filtering objectionable content, *Hoffberg* states:

> In the event that alternate material is unavailable, or the scene is critical to the performance, or information is unavailable, or otherwise, the content analysis aspects of the present invention may be employed to "censor" the content. For example, a "nudity" detector may be employed to monitor broadcasts for visual depictions of nudity, which would then be eliminated, and replaced with blurs or otherwise obscured. The semantic content (audio or textual) may also be monitored for profane language and eliminated. (This same type of semantic content analyzer may also provide language translation functionality, using a speech recognition system, with either a close caption translation or synthetic speech translation). In the case of less discrete objectionable content, such as violence or adult themes, such discrete censorship would be less effective. However, using artificial intelligence and/or metadata streams (including but not limited to EPG, MPEG 7, V-chip ratings, or the like) the system may be able to block presentation on a less granular basis. The system may also provide a reporting system, wherein the controlling entity may define processing rules for common circumstances, either prospectively in the abstract or based on actual events stored in a buffer. Thus, the system may learn desired strategies for handling content issues, without requiring predefined deterministic algorithms.

Hoffberg, col. 223, line 66, to col. 224, line 22. Thus, *Hoffberg* appears to teach censoring content if nudity or other objectionable content can be detected. However, *Hoffberg* teaches an all-or-nothing approach to censoring objectionable content. There is no teaching in *Hoffberg* of a **plurality of thresholds** for a **plurality of categories** of objectionable content.

Also, *Hoffberg* appears to teach a composite score, as acknowledged in the Final Office Action. However, this actually teaches away from the presently claimed invention, because the analysis of *Hoffberg* results in a single score, rather than analyzing content based on a plurality of

thresholds. The single composite score of *Hoffberg* leads to the all-or-nothing approach, which is not equivalent to the presently claimed invention. That is, *Hoffberg* does not allow for a low threshold for nudity and a high threshold for violence, for example.

Furthermore, *Jensen* also fails to teach the limitations of the present invention. For example, *Jensen* does not teach or suggest determining a score for requested content for each of a plurality of categories of objectionable content. *Jensen* makes no mention of a score. In fact, the word "score" does not even appear in the reference. The semantic value is not a score that is compared to a threshold, as in the presently claimed invention. Rather, the semantic value of *Jensen* is analogous to a fingerprint, a piece of data that is used to identify something. The semantic value of *Jensen* is not indicative of an amount of objectionable content, as recited in claim 1, for example.

The applied references do not teach or suggest each and every claim limitation; therefore, *Hoffberg* and *Jensen*, taken alone or in combination, do not render claim 1 obvious, for example. Independent claims 17 and 33 recite subject matter addressed above with respect to claim 1 and are allowable for similar reasons. Since claims 3-6, 10, 11, 16, 19-22, 26, 27, 32, 35-38, 42, 43, and 48 depend from claims 1, 17, and 33, the same distinctions between *Hoffberg* and *Jensen* and the invention recited in claims 1, 17, and 33 apply for these claims. Additionally, claims 3-6, 10, 11, 16, 19-22, 26, 27, 32, 35-38, 42, 43, and 48 recite other additional combinations of features not suggested by the references.

Therefore, Appellants respectfully request that the rejection of claims 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48 under 35 U.S.C. § 103(a) not be sustained.

IA. <u>35 U.S.C. § 103, Alleged Obviousness of claims 11, 16, 27, 32, 43, and 48</u>

Claims 16, 32, and 48, which depend from claims 3, 19, and 35, respectively, recite determining a new value for the at least one predetermined threshold using one of an algorithm, a function, an inference engine, a neural network, an expert system, or an intelligent computing system. The Office Action alleges that *Hoffberg* and *Jensen* teach this feature. However, *Hoffberg* and *Jensen* fail to teach a plurality of thresholds for a plurality of categories of objectionable content. Therefore, *Hoffberg* and *Jensen* cannot teach the further limitation of determining a **new** value for at least one of the plurality of thresholds. Claims 11, 27, and 43 are

allowable for similar reasons.

Therefore, Appellants respectfully request that the rejection of claims 11, 16, 27, 32, 43, and 48 under 35 U.S.C. § 103(a) not be sustained.

IB. 35 U.S.C. § 103, Alleged Obviousness of claims 10, 26, and 42

With respect to claims 10, 26, and 42, the Office Action alleges that *Jensen* teaches thresholds being dynamically adjustable because *Jensen* teaches that archetypes may be updated at col. 11, lines 56-57. Appellants respectfully disagree. Simply stated, an archetype is not a threshold that is compared to a score that is indicative of an amount of objectionable content, as recited in the instant claims. The applied reference clearly fails to teach or suggest all limitations of instant claims; therefore, *Hoffberg* and *Jensen* do not render claims 10, 26, and 42 obvious.

Therefore, Appellants respectfully request that the rejection of claims 10, 26, and 42 under 35 U.S.C. § 103(a) not be sustained.

CONCLUSION

In view of the above, Appellants respectfully submit that claims 1, 3-6, 10, 11, 16, 17, 19-22, 26, 27, 32, 33, 35-38, 42, 43, and 48 are allowable over the cited prior art and that the application is in condition for allowance. Accordingly, Appellants respectfully request the Board of Patent Appeals and Interferences to not sustain the rejections set forth in the Final Office Action.

Stephen R. Tkacs
Reg. No. 46,430
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal reads:

1. A method of identifying objectionable content, comprising:

receiving requested content;

retrieving a user profile for a requesting user, wherein the user profile includes parameters for identifying objectionable content and a plurality of thresholds including a threshold for each of a plurality of categories of objectionable content;

analyzing the requested content using the parameters stored in the user profile of the requesting user to identify an amount of objectionable content based on the parameters for each of the plurality of categories of objectionable content;

determining a score for the requested content for each of the plurality of categories of objectionable content based on the amount and category of objectionable content contained in the requested content; and

storing the requested content in an objectionable content data structure if a score for the requested content is above at least one threshold for at least one category of objectionable content.

3. The method of claim 1, further comprising:

providing at least one entry from the objectionable content data structure to a user;

receiving input from the user categorizing the at least one entry as objectionable or non-objectionable; and

adjusting at least one predetermined threshold within the plurality of thresholds if the input from the user categorizes the at least one entry as non-objectionable.

4. The method of claim 1, wherein the method is implemented in a proxy server.

5. The method of claim 1, wherein the method is implemented in a client device.

6. The method of claim 1, wherein analyzing the requested content to identify an amount of objectionable content includes one or more of performing image analysis, performing list based analysis, performing textual analysis, or receiving an input from a user designating the requested content as containing objectionable content.

10. The method of claim 1, wherein the plurality of thresholds are dynamically adjustable.

11. The method of claim 1, wherein the plurality of thresholds are dynamically adjustable based on results of review, by a user, of objectionable content in the objectionable content data structure.

16. The method of claim 3, wherein adjusting the at least one predetermined threshold if the input from the user categorizes the at least one entry as non-objectionable includes determining a new value for the at least one predetermined threshold using one of an algorithm, a function, an inference engine, a neural network, an expert system, or an intelligent computing system.

17. An apparatus for identifying objectionable content, comprising:

a first interface which receives requested content;

a user profile for a requesting user, wherein the user profile stores parameters for identifying objectionable content and a plurality of thresholds including a threshold for each of a plurality of categories of objectionable content;

a processor which analyzes the requested content using the parameters stored in the user profile of the requesting user to identify an amount of objectionable content based on the parameters for each of the plurality of categories of objectionable content and determines a score for the requested content for each of the plurality of categories of objectionable content based on the amount and category of objectionable content contained in the requested content; and

a storage device which stores the requested content in an objectionable content data structure if a score for the requested content is above at least one threshold for at least one category of objectionable content.

19. The apparatus of claim 17, further comprising:

a second interface which provides at least one entry from the objectionable content data structure to a client device; and

a third interface which receives input from a user categorizing the at least one entry as objectionable or non-objectionable, wherein the processor adjusts at least one predetermined threshold within the plurality of thresholds if the input from the user categorizes the at least one entry as non-objectionable.

20. The apparatus of claim 17, wherein the apparatus is a proxy server.

21. The apparatus of claim 17, wherein the apparatus is a client device.

22. The apparatus of claim 17, wherein the processor performs one or more of image analysis, list based analysis, or textual analysis to identify an amount of objectionable content.

26. The apparatus of claim 17, wherein the plurality of thresholds are dynamically adjustable.

27. The apparatus of claim 17, wherein the plurality of thresholds are dynamically adjustable based on results of review, by a user, of objectionable content in the objectionable content data structure.

32. The apparatus of claim 19, wherein the processor determines a new value for the at least one predetermined threshold using one of an algorithm, a function, an inference engine, a neural network, an expert system, or an intelligent computing system.

33. A computer program product in a computer readable medium for identifying objectionable content, comprising:

instructions for receiving requested content;

instructions for retrieving a user profile for a requesting user, wherein the user profile includes parameters for identifying objectionable content and a plurality of thresholds including a threshold for each of a plurality of categories of objectionable content;

instructions for analyzing the requested content using parameters stored in a user profile of the requesting user to identify an amount of objectionable content based on the parameters for

each of the plurality of categories of objectionable content;

instructions for determining a score for the requesting content for each of the plurality of categories of objectionable content based on the amount and category of objectionable content contained in the requested content; and

instructions for storing the requested content if a score for the requested content is above at least one threshold for at least one category of objectionable content.

35. The computer program product of claim 33, further comprising:

instructions for providing at least one entry from the objectionable content data structure to a user;

instructions for receiving input from the user categorizing the at least one entry as objectionable or non-objectionable; and

instructions for adjusting at least one predetermined threshold within the plurality of thresholds if the input from the user categorizes the at least one entry as non-objectionable.

36. The computer program product of claim 33, wherein the computer program product is executed in a proxy server.

37. The computer program product of claim 33, wherein the computer program product is executed in a client device.

38. The computer program product of claim 33, wherein the instructions for analyzing the requested content to identify an amount of objectionable content includes instructions for performing one or more of image analysis, list based analysis, or textual analysis.

42. The computer program product of claim 33, wherein the plurality of thresholds are dynamically adjustable.

43. The computer program product of claim 33, wherein the plurality of thresholds are dynamically adjustable based on results of review, by a user, of stored objectionable content.

48. The computer program product of claim 35, wherein the instructions for adjusting the at least one predetermined threshold if the input from the user categorizes the at least one entry as non-objectionable includes instructions for determining a new value for the at least one predetermined threshold using one of an algorithm, a function, an inference engine, a neural network, an expert system, or an intelligent computing system.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.